# EOSDIS Element Name

**INFORMATION TECHNOLOGY (IT)**

**SECURITY PLAN FOR**

**(GENERAL SUPPORT SYSTEM TITLE)**

**(TEMPLATE)**

**Organization Title and Code**

**Month, Year**

**Administratively Controlled Information**

This document contains sensitive information and shall be handled in a way that precludes its disclosure to the general public and limits its circulation. NASA entities must attach the NASA Form 1686, Administratively Controlled Information (ACI) form to the cover of this document.

# EOSDIS Element Name

## INFORMATION TECHNOLOGY (IT) GENERAL SUPPORT SYSTEMS SECURITY PLAN (TEMPLATE)

**Organization Title and Code**

**Prepared by:**

(Name) Date
(Title)
(Organization)

**Reviewed by:**

(Name) Date
(Title)
(Organization)

**Approved by:**

(Name) Date
(Title)
(Organization)

This page intentionally left blank

# Preface

This security plan provides an overview of the security requirements of the (element) (system name) and describes the controls in place or planned for meeting the requirements. It delineates the responsibilities and expected behavior of all individuals who access the system.

Proposed changes to this document shall be submitted to the ESDIS Computer Security Official (ECSO) along with supporting materials justifying the proposed revision. These changes will be issued by Documentation Change Notice (DCN), or where applicable, by complete revision.

Questions concerning this document and proposed changes shall be addressed to:

Clayton Sigman
ESDIS IT Security Official
NASA GSFC Code 423
Greenbelt, MD 20771

(301) 614-5309
Clayton.Sigman@gsfc.nasa.gov

# Change Information Page

| Issue | Date | Pages Affected | Description |
|---|---|---|---|
| Original | | | |

This page intentionally left blank

# List of Affected Pages

| Page No. | Revision | Page No. | Revision | Page No. | Revision | Page No. | Revision |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

This page intentionally left blank.

# Table of Contents

## SECTION 1. SYSTEM IDENTIFICATION



## SECTION 2. Information Identification



## SECTION 3. INFORMATION SHARING



## SECTION 4. RISK ASSESSMENT AND ANALYSIS



## SECTION 5. TECHNICAL CONTROLS

## SECTION 6. PUBLIC ACCESS CONTROLS



## SECTION 7. RULES OF THE SYSTEM



## SECTION 8. PERSONNEL SCREENING



## SECTION 9. SPECIALIZED TRAINING

## SECTION 10. CONTINGENCY PLANNING



## SECTION 11. INCIDENT RESPONSE



## SECTION 12. SYSTEM INTERCONNECTION



## SECTION 13. REVIEW OF SECURITY CONTROLS



## SECTION 14. AUTHORIZATION TO PROCESS

# Section 1. System Identification

## 1.1 Responsibilities

### 1.1.1 Organization

In this section, list the federal organizational sub-component responsible for the system. If a state or local government or contractor performs the function, identify both the federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Include physical locations and addresses, as well as the organizational point of contact for the application. Identify any contractual agreements or memorandums of understanding.

Example: NASA
Goddard Space Flight Center
Greenbelt, MD 20662-1010

This system is maintained by:

Raytheon, Inc.
12345 Westpoint Rd.
Toronto, Canada

### 1.1.2 Manager

Identify the management official responsible for the security of the system.

## 1.2 System Identification

Each system/application should be assigned a unique name/identifier

- Provide the Unique Identifier & Name Given to the System

## 1.3 Special Management Attention

If the system has been identified as needing "special management", select one of the following and describe the reasons special management attention is required.

- Major Information System. A system that has been designated as a "major information system for OMB A-11 reporting.
- Mission Critical System. A system that provides agency-wide support, such as a wide area network, agency-wide business function, command control of space system, agency-wide consolidated computer resource, or computer resource that affects life support.
- NASA Resource Protection (NRP) Facility. A computer resource that is critical to a facility or operation as designated under the NRP program by the cognizant Program Office (Reference: NPD 1600.2 NASA Security Program.)

- Other Designated. Other computer systems that have been designated as requiring special management attention.

## 1.4 Operational Status

In this section, determine which phase(s) of the life cycle the system, or parts of the system, are in. Identify how security has been handled during the applicable life cycle phase. Listed below is a description of each phase of the life cycle, which includes questions that will prompt the reader to identify how security has been addressed during the life cycle phase(s) that the major application or general support system is in. There are many models for the IT system life cycle but most contain five basic phases: Initiation, development/acquisition, implementation, operation, and disposal.

- Determine which phase(s) of the life cycle the system, or parts of the system are in.
- Describe how security has been handled in the life cycle phase(s) the system is currently in.

Phase Descriptions:

**A. Initiation Phase**. During the initiation phase, the need for a system is expressed and the purpose of the system is documented. A sensitivity assessment can be performed which looks at the sensitivity of the information to be processed and the system itself.

- Reference the sensitivity assessment that is described in Section 2.2, Information Category and Sensitivity.

**B. Development/Acquisition Phase**. During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

During the first part of the development/acquisition phase, security requirements should be developed at the same time system planners define the requirements of the system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). If the system or part of the system is in this phase, include a general description of any specifications that were used and whether they are being maintained. Among the questions that should be addressed are the following:

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new

threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

**C. Implementation Phase**. In the implementation phase, the system's security features should be configured and enabled, the system should be tested and installed or fielded, and the system authorized for processing. A design review and systems test should be performed prior to placing the system into operation to assure that it meets security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed. This ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the official organization records.

If the system or parts of the system are in the implementation phase, describe when and who conducted the design reviews and systems tests. Include information about additional design reviews and systems tests for any new controls added after the initial acceptance tests were completed. Discuss whether the documentation of these reviews and tests have been kept up-to-date and maintained in the organization records.

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

**D. Operation/Maintenance Phase**. During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. If the system is undergoing modifications, determine which phase of the life cycle the system modifications are in and describe the security activities conducted or planned for in that part of the system. For the system in the operation/maintenance phase, this security plan should be documenting the security activities in other sections.

- This security plan documents the security activities required for this phase.

**E. Disposal Phase**. The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software. If the system or part of the system is at the end of the life cycle, briefly describe in this section the following:

- Information. Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the

information in the future. While electronic information is generally easier to retrieve and store, the technology used to create the records may not be readily available in the future. Measures may also have to be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is important to consider legal requirements for records retention when disposing of IT systems. For federal systems, system management officials should consult with their office responsible for retaining and archiving federal records.

- Media Sanitization. The removal of information from a storage medium (such as a hard disk or tape) is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by keyboard attack) and purging (rendering information unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing (for magnetic media only), and destruction.

## 1.5 General Description/Purpose

1.5.1 Present a brief description (one-three paragraphs) of the function and purpose of the system (modeling, simulation, accounting, satellite weather data processing and analysis). Include:

- Major uses or functions
- Network access and connectivity (provide a network diagram as an attachment.)
- Operated by government or contractors.
- Hours of operation.
- Number of user accounts and types of users (e.g., researchers, programmers, administrative support)

1.5.2 List the make and model of major hardware components.

1.5.3 List all system software and versions and the software applications running on the general support system. Specify if the application is or is not a major application and include unique name/identifiers where applicable. Describe each application's function and the information processed.

## 1.6 Processing Environment and Special Considerations

Provide a brief general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- Critical processing periods (e.g., end of month, pay day)

- Indication of whether the system serves a large number of offsite users, such as university students, other agencies, or foreign nationals.
- Identify whether the system is connected to the Internet.
- Describe other systems/applications that interface with the system.

## 1.7 Information Contacts

Provide the names, telephone numbers, mailing addresses and electronic mail address for each of the following individuals:

A. Element Manager
B. Computer Security Point of Contact
C. System Administrator
D. Other technical contacts (e.g., staff who support the system administrator)

# Section 2. Information Identification

## 2.1 Information Processed

Describe in detail the information processed. Include a processing flow diagram of the application from system input to system output

## 2.2 Information Category and Sensitivity

All information stored, processed, or transmitted by EOSDIS' information systems is sensitive to some degree and is entitled to some degree of protection. Various categories of information should be protected using different means, stringency levels, and controls according to the risk and impact of their being altered, destroyed, made unavailable, or disclosed. NASA classifies information such that the information used in conducting daily business falls into five categories:

A. **Mission (MSN) Information**: If the information, software applications, or computer systems in this category are altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency mission. Examples in this category are those that control or directly support one of the following:
   (1) Human space flight.
   (2) Wide Area Networks
   (3) Development of the data or software used to control human flight
   (4) Training simulation vehicles
   (5) Wind tunnel operations
   (6) Launch operations
   (7) Space vehicle operations

B. **Business and Restricted Technology (BRT) Information**: This category consists of information that NASA is required by law to protect. It includes information, software applications, or computer systems that support the Agency's business and technological needs. In general, if information in this category should be disclosed inappropriately, the disclosure could result in damage to our employees, in loss of business for our partners and customer businesses, in contract protest, or the illegal export of technology. This category includes systems containing technological information that is restricted from general public disclosure because of public laws. Examples in this category are those that are related to the following kinds of information:
   (1) Financial
   (2) Legal
   (3) Payroll
   (4) Personnel

(5) Procurement
(6) Source selection
(7) Proprietary information entrusted to the Government
(8) Export controlled technical information (includes disclosure to foreign nationals)

C. **Scientific, Engineering, and Research (SER) Information**: All official NASA information may be released publicly only in accordance with NASA regulations; however, systems in this category do not contain information for which the release is otherwise governed by law. This category consists of information that supports basic research, engineering, and technology development but is less restricted against public disclosure.

Alteration, destruction, unauthorized disclosure, or unavailability of the systems, application, or information would have an adverse or severe impact on individual projects, scientists, or engineers; however, recovery would not impede the accomplishment of a primary mission.

Integrity is the driving concern in this category followed by availability. Confidentiality is important and should be considered in a risk assessment insofar as it protects individual researchers from such things as premature disclosure of their work by another party. The impact, however, is primarily on an individual.

D. **Administrative (ADM) Information**: Administrative Information includes, but is not limited to electronic correspondence, briefing information, project/program status, infrastructure design details, predecisional notes, vulnerability descriptions, passwords, and internet protocol addresses. Organizations run various applications—from problem reports to configuration management tools—on administrative IT systems.

This category includes systems, applications, and information that support daily activities, such as electronic mail, forms processing, networking, and management reporting.

Integrity and availability are the driving IT security concerns. The impact is primarily managerial in nature, which would require time and resources to correct. Confidentiality may be of concern in certain specific administrative information. In such instances, additional security controls must be imposed as a risk analysis dictates.

E. **Public Access (PUB) Information**: This category includes information, software applications, and computer systems specifically intended for public use or disclosure, such as a public web site or hands-on demonstrations. The loss, alteration, or unavailability of information in this category would have little direct impact on NASA's missions but might expose the Agency to embarrassment, loss of credibility, or public ridicule.

Information posted for public access which could expose NASA missions to risk if compromised should be afforded additional protective measures. In these cases, the baseline requirements for ADM information should be implemented. (For example, contractors may submit proposals based on information from NASA web sites. Loss, alteration, or unavailability of data at the site could result in protests, thereby impacting procurement cycle time and ultimately NASA missions.)

Integrity and availability are the driving concerns. IT security controls are selected to protect the resources themselves and are not intended to protect the confidentiality of the information.

## 2.3 Applicable Laws, Policies and Guidance Affecting the Information

List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of data/information in the system. Each organization should decide on the level of laws, regulations, and policies to include in the security plan. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information). If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities. Include NASA and Center policies in the list.

*Examples: Privacy Act of 1974 (PL-93-579)*
*Paperwork Reduction Act of 1980 as amended in 1995*

## 2.4 Impact of Loss of System or Data

Describe the potential impacts if the system, application, or the information processed is altered, destroyed or unavailable (i.e., at what point does the loss become a high priority – 1 hour, 1 day, 1 week, or 1 month?). Describe the need for protective measures. Relate the information handled to each of the three basic protections requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: High, Medium, or Low.

- *High* – a critical concern of the system;
- *Medium*– an important concern, but not necessarily paramount in the organization's priorities; or
- *Low* – some minimal level or security is required, but not to the same degree as the previous two categories.

*Example 1: This application has been evaluated as mission essential information (MSN) since it is used to support manned space flights. A high degree of security for the system is considered mandatory to protect the confidentiality, integrity, and*

*availability of information. The protection requirements for all applications are critical concerns for the system, since failure could result in the loss of human life. During a manned space flight mission, loss of the system at any time is critical.*

*Example 2: Confidentiality is not a concern for this system as it contains information intended for immediate release to the general public (PUB) concerning severe storms. The integrity of the information, however, is extremely important to ensure that the most accurate information is provided to the public to allow them to make decisions about the safety of their families and property. The most critical concern is to ensure that the system is available at all times to acquire, process, and provide warning information immediately about life-threatening storms.*

Discuss the loss of data, loss of processing time, recovery cost for hardware and software (i.e., programs), impact to budgets, impact to customers, and estimated recovery time.

## 2.5 System Value

Estimate the replacement cost for the hardware and software programs that comprise the system. Be sure to include the cost of rebuilding databases and programming code if they are not backed up or they are not remotely located. Note: If the Risk Assessment is attached to this security plan, reference the appropriate section if desired.

# Section 3. Information Sharing

## 3.1 External Customers

Identify external customers and the information and processing to be shared with them. External customers are any federal, state, or local governments, other NASA organizations, international partners, or organizations in the private sector. Identify the controls that will be used for each of the intended recipients.

## 3.2 Applicable Policies and Laws to Protect Shared Information

Identify any applicable policies or laws that must be followed. Include identification of any Memorandums of Understanding.

# Section 4. Risk Assessment and Analysis

The NPG 2810.1 requires an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. The methods used to assess the nature and level of risk to the system should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

## 4.1 Risk Assessment Summary

Summarize the findings of the risk assessment performed on the system. Include the Risk Assessment Plan as an attachment. Identify when the risk assessment was done, who conducted it, and who approved it. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

## 4.2 Risk Assessment Results

Describe any findings or recommendations from the assessment and include information concerning correction of any deficiencies of completion of any recommendations. Describe any residual risks and indicate the possible effects these risks could have.

## 4.3 Baseline Requirements

Document any baseline requirements that are not being met and indicate why the requirement is not being met or why it is not applicable. (See Appendix A to this template for the list of baseline requirements).

# Section 5. Technical Controls

Security controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise, and often rely upon management activities as well as technical controls. In this section, describe the measures (in place or planned) that are intended to meet the protection requirements of the system. Attachment A of this template identifies controls that NASA has determined will sufficiently protect different information categories/sensitivity levels of information.

## 5.1 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics which are explained below. In this section, briefly describe the physical and environmental controls in place for the major application.

- Discuss the physical protection and access controls in the area where application processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.).
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.

*Example:* ***In Place***

*Card keys for building and work-area entrances*
*Twenty-four hour guards at all entrances/exits*
*Cipher lock on computer room door*
*Raised floor in computer room*
*Dedicated cooling system*
*Humidifier in tape library*
*Emergency lighting in computer room*
*Four fire extinguishers rated for electrical fires*
*One B/C-rated fire extinguisher*
*Smoke, water, and heat detectors*
*Emergency power-off switch by exit door*
*Surge suppressor*
*Emergency replacement server*
*Zoned dry pipe sprinkler system*
*Uninterruptable power supply for LAN servers*
*Power strips/suppressors for peripherals*
*Power strips/suppressors for computers*
*Controlled access to file server room*

***Planned***

*Plastic sheets for water protection, December 2000*
*Closed circuit television monitors, January 2001*

## 5.2 Production, Input/Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, application software should be listed. In this section, provide a synopsis of the procedures in place that support the operations of the application. Below is a sampling of topics that should be reported in this section.

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Audit trails for receipt of sensitive inputs/outputs.
- Procedures for restricting access to output products.
- Procedures and controls used for transporting or mailing media or printed output.
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary).
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).
- Audit trails for inventory management.
- Media storage vault or library-physical, environmental protection controls/procedures.
- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing).
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.
- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

## 5.3 Hardware and System Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, hardware, operating system software, and other software to ensure that the hardware and software function as expected, and that a historical record is maintained of application changes. These controls may also be used to ensure that only authorized software is installed on the system. Such controls may include a hardware and software configuration policy that grants managerial approval (re-authorize processing) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for, or preventing, illegal use of shareware or copyrighted software. In this section, provide several paragraphs on the hardware and system software maintenance controls in place or

planned. The following statements are examples of items that should be addressed in responding to this section:

- Restriction/controls on those who perform maintenance and repair activities.
- Special procedures for performance of emergency repair and maintenance.
- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
- Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.
- Version control that allows association of system components to the appropriate system version.
- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
- Change identification, approval, and documentation procedures.
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
- Are test data "live" data or made-up data?.
- Are there organizational policies against illegal use of copyrighted software or shareware?

## 5.4 Integrity Controls

Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered.

In this section, describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected. The following questions are examples of some of the controls that fit in this category:

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Is reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Is password crackers/checkers used?
- Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?

- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission?

## 5.5 Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

*Example:*
- *Vendor-supplied documentation of hardware*
- *Vendor-supplied documentation of software*
- *Security plan*
- *General support system security plan*
- *Testing procedures and results*
- *Standard operating procedures*
- *Emergency procedures*
- *Contingency/Disaster recovery plans*
- *User rules of behavior*
- *User manuals*
- *Risk assessment*
- *Backup procedures*
- *Verification reviews/site inspections*

## 5.6 Identification and Authentication

Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

- Describe the method of user authentication (password, token, and biometrics)
- If a password system is used, provide the following specific information
- Allowable character set
- Password length (minimum, maximum)

- Password aging time frames and enforcement approach
- Number of generations of expired passwords disallowed for use
- Procedures for password changes
- Procedures for handling lost passwords
- Procedures for handling password compromise
- Procedures for training users and the materials covered
- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
- Describe any token controls used on this system and how they are implemented.
- Describe the level of enforcement of the access control mechanism (network, operating system, and application).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).
- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
- If digital signatures are used, the technology must conforms with FIPS 186, *Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures.

## 5.7 Logical Access Controls

Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

In this section, identify the controls in place to authorize or restrict the activities of users and system personnel within the general support system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). The following are areas that should be considered.

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the application. Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists [ACLs).
- How are access rights granted? Are privileges granted based on job function?
- Describe the application's capability to establish an ACL or register.
- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application accesses control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

## 5.8 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. In this section, describe the audit trail mechanisms in place. A list of items to consider are provided below:

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event

occurred, user id associated with the event, program or command used to initiate the event.)

- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if, for examples, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.
- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?
- If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users. The Rules of Behavior may be one vehicle for distributing the information. If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the Department of Justice has reviewed the policy.

# Section 6. Public Access Controls

## 6.1 Public Access Controls

If general public access is allowed, discuss the additional security controls used to protect the information, software applications, and systems against loss, alteration, unavailability, or unauthorized disclosure, as appropriate. Such controls include segregating information made directly accessible to the public from official agency records. Others might include:

- Some form of identification and authentication
- Access control to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information on the system
- Digital signatures
- CD-ROM for on-line storage of information for distribution
- Put copies of information for public access on a separate system
- Prohibit public to access “live” databases
- Verify that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- System and data availability
- Legal considerations

# Section 7. Rules of the System

Attach the rules of behavior for the system as an appendix and reference the appendix number in this section, or insert the rules into this section. A set of rules of behavior must be established for each system. The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains. The acceptable level of risk should form the basis for determining the rules.
The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt. A sample Rules of Behavior is included as Attachment B of this template. The rules should cover matters such as the following:

## 7.1 Process of Obtaining an Account

Identify the process for obtaining an account.

## 7.2 Process for Remote Access

Identify the process for accessing the system from home or while on travel/dial-in access.

## 7.3 Connection to the Internet

Identify rules for Internet use.

## 7.4 Use of Copyrighted Works

Identify rules about using copyrighted software and applications.

## 7.5 Unofficial Use of Government Equipment

Identify rules about unofficial use of government equipment.

## 7.6 System Information Storage and Authorized Uses.

Identify the types of information that may be stored on the system and the authorized uses to which that information may be put.

## 7.7 User Privileges and Limitations

Identify for privileged and non-privileged users.

## 7.8 User Authentication

Rules regarding password use should be consistent with technical password features in the system.

## 7.9 Process for Restoring Service From Crashes or Maintenance

Identify the process for restoring service from system crashes or maintenance.

## 7.10 Process for Escorting/Monitoring Personnel

Identify the process escorting/monitoring personnel.

## 7.11 Individual Accountability

Identify whether individuals are held accountable for following the rules of the system.

## 7.12 Consequences for Failure to Follow Rules

Identify the consequences for failure to follow the rules of the system.

# Section 8. Personnel Screening

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change, then installs the program into the production environment without testing).

## 8.1 Screening Requirements

In this section, include detailed information about the following personnel security measures. It is recommended that most of these measures be included as part of the Rules of Behavior. If they are incorporated in the Rules of Behavior, reference the applicable section. If differences exist between requirements for privileged and limited privileged users, so specify. The NPG 2810.1, paragraph 4.5, provides guidance on Personnel Screening.

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned?
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

## 8.2 Privileged Accounts

Identify the number of privileged and limited privileged users who are able to bypass security process and controls.

# Section 9. Specialized Training

The NPG2810.1 requires mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This includes contractors as well as employees of the agency. OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user must be versed in acceptable rules of behavior for the application before being allowed access to the system. The training program should also inform the user on how to get help when having difficulty using the system and procedures for reporting security incidents.

Access provided to members of the public should be constrained by controls in the applications, and training should be within the context of those controls and may consist only of notification at the time of access.

## 9.1 Security Awareness Program

Describe the awareness program for the application (posters, booklets, and trinkets). (NPG 2810.1, paragraph 4.3, provides guidelines for IT security awareness and training.) The awareness program should include at least the following:

- Organizational responsibilities
- Rules of the system
- How to detect and respond to suspected IT security incidents
- How to get help in using the system and its security features
- Element's policies, procedures, and guidelines

## 9.2 Training Frequency

Describe the type and frequency of application-specific and general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training).

## 9.3 Training Assurance

Describe the procedures for assuring that employees and contractor personnel have been provided adequate training.

# Section 10. Contingency Planning

A plan for continuing operations in the case of a natural or human-caused disaster must be established and tested. If one or more applications are run in a system furnished by another organization, the application manager's job is to plan how the application will continue performing its critical functions if the facility where processing normally occurs suddenly becomes unable to support the application.

## 10.1 Contingency Plan

At the manager's option, depending upon the size and complexity of the system, the contingency plan may be described in this section. If the contingency plan exists as a separate document, it may be referenced in this section and attached as an appendix.

## 10.2 Testing and Training

Identify how often the contingency/disaster recovery plan is tested and the date last tested. Describe how employees are trained in their roles and responsibilities relative to the plan.

## 10.3 Processing Restoral

Indicate the estimated time required to return to full processing capability.

## 10.4 Backup Procedures

Include descriptions for the following:

- Any agreements of backup processing.
- Documented backup procedures, including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup).
- Location of stored backups and generations of backups.

# Section 11. Incident Response

A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or threatened breach of these mechanisms. Computer security incidents are becoming more common and their impact far-reaching. When faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. The NPG 2810.1 requires each agency to ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.

## 11.1 Handling Procedures

In this section, describe the incident handling procedures in place for the general support system.

- Are there procedures for reporting incidents handled either externally or by system personnel?
- Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?
- What preventative measures are in place, i.e., intrusion detection tools, automated audit logs, penetration testing?

## 11.2 Reporting Procedures

Identify the names and telephone numbers of people who should be called if a security incident is discovered. If special incident response procedures are required, include them in this section.

# Section 12. System Interconnection

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to effect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

## 12.1 System Interconnectivity

List interconnected systems and system names and identifiers (if appropriate), including Internet. Identify the organization owning the system. Identify the type of interconnection (TCP/IP, Dial, SNA, etc.). Discuss how the access to and from other systems is controlled to an acceptable degree of risk. If users of this system have limitations to external access, such as the Internet, these limitations should be described in this section and should be consistent with the system rules.

## 12.2 Interconnection Security Concerns

If connected to an external system not covered by a security plan, provide a short discussion of any security concerns that need to be considered for protection.

## 12.3 Interconnection Authorization

Describe the coordination that has taken place with other managers who share common resources. Describe the rules required for interconnection.

# Section 13. Review of Security Controls

The NPG 2810.1 requires that at least every three years, or upon significant change, an independent review of the security controls for each major application be performed

## 13.1 Security Audit/Review Process

Describe the process for performing an independent review of the security controls of the system.

# Section 14. Authorization to Process

The term “authorize processing” is the authorization granted by a management official for a system to process information. Authorization provides a form of quality control and is required by the NPG 2810.1This authorization must clearly state that the manager finds that the IT Security Plan adequately secures the major application, its data, and its operation, i.e. risk assessments, contingency plans, Rules of Behavior, etc. The authorization can be a cover letter attached to the plan or a signed statement at the end of this document. If this element is located at a NASA center, the Center CIO must also sign the authorization to process letter. A sample of an Authorization Letter is included as Attachment C to this template.

## 14.1 Authorizing Official

Provide the date of authorization, name, and title of the management official authorizing processing of the system. If not authorized, provide the name and title of manager requesting approval to operate and the date of the request.

# Attachment A: Baseline Information Technology (IT) Security Requirements

1. The following security control items list the minimum technical, procedural, and physical IT security baseline requirements for protecting IT resources, and are required by the NPG 2810.1. These requirements will help managers determine the controls that are needed for computer systems under their oversight. They are intended to ensure a reasonable level of security for a system and are derived from "best practices" used by industry and the Government.

2. Baseline requirements are used in security planning as a benchmark for identifying risks to which a system may be exposed. The degree of compliance with these requirements is indicated in the IT Security Plan for the system. These requirements should also be used in the definition phase of the system life-cycle process to ensure that an acceptable level of security is built into a system.

3. Baseline requirements vary depending on the information category of the system. This attachment has been arranged in such a way that, based upon the information category (sensitivity level) determined for Section 2.2 of this security plan template, the baseline requirements identify the section of the template in which they would be discussed.

4. The requirements for each information category/sensitivity level are broken down into three parts; servers and mainframes, multiuser workstations, and singleuser workstations

## Baseline Security Requirements for Systems Rated Mission Essential (MSN)

# I. Servers and Mainframes

**Critical System Files Protection:** Critical system files are those that are integral to the operating system, system security mechanisms, or key system services. Corrupting these files would damage the integrity of the system.

**Template Section 5.7**

**Security Requirements**

- A list of authorized users of critical system files is maintained and verified at least semiannually.
- Configuration control is implemented for critical system files.
- Critical system file protection is reviewed at least semiannually.
- Access to password files is restricted to user ID management personnel.
- Access to critical system files are restricted to a minimum number of authorized system support personnel.
- Critical system files are identified and protected.
- File access is controlled.

**Privileged Users and Programs:** A privileged user is one who can alter or circumvent the operating system or the system's security privileges. A privileged program may have the capability to override or bypass security measures when executed. It is vital to monitor privileged access.

**Template Section 5.7**

**Security Requirements**

- System administration/support personnel do not function as system auditors.
- A list of privileged users is maintained and verified at least semiannually.
- Operating system privileges are assigned to a minimum number of systems personnel.
- Access is controlled to privileged programs.

**Journaling and Monitoring:** Most multiuser computers have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or security problems.

**Template Section 5.8**

**Security Requirements**

- System journals record security-related events.
- Journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts.
- All file creation/modification/deletion events are recorded.
- Journals are reviewed daily or when problems are suspected.
- Successful and failed logons/logoffs are recorded.

**System Retention/Backup:** To ensure continuity of operation, copies of important software and data will be made and retained.

**Template Section 10**

**Security Requirements**

- The most recent, or most recent minus one, backup is stored external to the site.
- Operating system backups are retained for at least 1 year.
- Operating systems and key system services are backed up at least monthly and when modified.
- Journals are retained at least 1 year or 3 generations (whichever is longer).

**System Shutdown/Restart:** The system should provide security safeguards to cover unscheduled system shutdowns, (e.g., aborts) and subsequent restarts as well as for scheduled shutdowns and startups.

**Template Section 5.8**

**Security Requirements**

- All aborts and restarts are logged and documented.
- Only authorized personnel shutdown/restart the system.
- System shutdown/restart procedures are documented.

**Operating System Local Modifications:** Local modifications to the operating system can have security implications. If incorrectly designed or implemented, local operating systems modifications may invalidate the system's security controls.

**Template Section 5.3**

**Security Requirements**

- All operating system security modifications are documented.
- All operating system security modifications are reviewed and approved.
- All operating system modifications are tested and/or evaluated for impact on security before permanent installation.

**Configuration Management:** Because the operating system governs the security of the system, changes to the operating system, including new releases and updates, will be controlled and monitored.

**Template Section 5.3**

**Security Requirements**

- All operating system changes are tested and/or evaluated and documented.
- Change control for critical system files is documented.

**User ID Approval Process/Privileges:** A process must be put in place to ensure that all requests for user ID's are reviewed and approved by management. A list of personnel who are authorized to approve the user ID's will be furnished to the appropriate user-ID administrator.

**Template Sections 7 and 9**

**Security Requirements**

- The request for a user ID is approved by the employee's manager. (If the employee is a contractor or other non-NASA employee, the approval of the employee's NASA sponsor is also required.)

- Each employee submits a formal request to the appropriate administrator for a user ID, which indicates the category being requested, such as group, personal, privileged, project, application system service, or generic.
- The user ID is removed after 150 days if the password has not been changed after notification
- Group user ID's are restricted to the minimum number necessary to conduct system operations.
- The statement of responsibility is retained by user ID management for every active account.
- Personnel screening and IT security briefing is verified.
- All individuals assigned a user ID sign a statement of responsibility indicating their understanding for using and safeguarding the information to which he/she is granted access.

**Group User ID's:** Group user ID's are discouraged because individual accountability is lost. However, if the system is configured such that group user ID's must be used, approval processes must be put in place.

**Template Section 5.6**

**Security Requirements**

- Group user ID's are not provided without risk justification and concurrence from all functional mangers of the affected data and applications.

**User ID Revalidation:** Management will ensure that an inventory is maintained of all assigned user ID's.

**Template Section 5.6**

**Security Requirements**

- All group user ID's are revalidated at least annually.
- A statement of responsibility is on file for each person who has a group user ID.

**Disposition of Unused User ID's:** Management will ensure that proper disposition is made of all unused user ID's. User ID disposition uses password lifetime as the metric for user-ID-deletion decisions.

**Template Section 5.6**

**Security Requirements**

- The user ID is suspended after 60 days if the password has not been changed after notification.
- A user will be reminded to change his or her password for 30 days.

**User ID Reuse:** User ID's may be reassigned after removal from the system under the following condition(s).

**Template Section 5.6**

**Security Requirements**

- A user ID may be reassigned after a 90 day waiting period has elapsed after removal.
- A user ID may be reassigned after all access rights and privileges associated with the user ID have been removed.

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual is **terminated for cause of because of reduction in force.**

**Template Section 5.6**

**Security Requirements**

- The user ID is removed as soon as practical, but no later than the end of the day of termination.

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual **has resigned, received a change of job, or has retired**, and no longer requires access to the system to perform assigned duties.

**Template Section 5.6**

**Security Requirements**

- The user ID is removed within 2 working days.

**Individual Accountability**

**Template Section 7**

**Security Requirements**

- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.
- Individuals are held accountable for the protection against loss or disclosure of password they possess.

**Password Length and Composition**

**Template Sections 5.7 and 7**

**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**

**Template Sections 5.7 and 7**

**Security Requirements**

- The password is not the name of a vendor product or a nickname for a product.
- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.
- The password is not equal to the user ID.

**Password Maximum Lifetime**

**Template Sections 5.7 and 7**

**Security Requirements**

- The password expires after 30 days maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.
- Personal passwords are not shared.
- Group passwords are not allowed.

**Password Reuse**
**Template Sections 5.7 and 7**
**Security Requirements**

- The owner uses a minimum of 10 passwords before reuse.

**Password Storage**
**Template Section 5.7**
**Security Requirements**

- Stored passwords are protected in such a way that only the password system is authorized access to a password.
- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

**Password Distribution**
**Template Section 5.7**
**Security Requirements**

- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.
- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.
- Passwords are not visible at the user terminal when being typed.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.
- The password is reset by the user during the first sign-on.
- A new nontrivial password is assigned at the user's request.
- The policy ensures that positive identification of the user ID owner is provided.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password assignment is nontrivial.
- All vendor-supplied passwords are removed.
- The initial user password is changed during the first logon by the user.

**User Authentication: Local Logon (used to log on directly to a system) :** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- User identification and local authentication (at least passwords) is required for all user ID's.

**User Authentication: Remote Logon (access a second system from the first without invoking a second authentication):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- Remote authentication is permitted at the discretion of the remote system admin when the authenticating system meets all security requirements of the remote system, audit trails are created, and the risk of subverting the connection is acceptable.

**Failed Logon Attempts:** Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination. Excessive failed logon attempts may indicate that an unauthorized user is attempting to access the system.
**Template Section 5.7 and 5.8**
**Security Requirements**

- The user ID is suspended, by system intervention, after three or fewer unsuccessful logon attempts or provides some form of system evasive action.
- The system notifies the System Administrator of user ID suspensions.
- The log of unsuccessful logon attempts is reviewed daily.
- The user ID owner is notified of failed logon attempts.

**Controlled Access Protection:** Controlled access protection is the ability of the system to control which users have access to resources. Ensure that all systems accessed will provide controlled access protection when users are not authorized for all information on the system.
**Template Sections 5.7 and 5.8**
**Security Requirements**

- The system provides individual electronic accountability through identification and authentication of each system user.

- The system provides the ability to control a user's access to information.
- The system provides audit trails or a journal of security-relevant events.

**Default File Protection:** Default file protection is the access control the system places on a file when the data owner does not take explicit action.

**Template Section 5.7**

**Security Requirements**

- System default file protection parameters are set to prevent read and execute access by anyone except the file owner and necessary operating system components.
- System default file protection parameters are set to grant write access to the file owner and to necessary operating system components.

**Data Owner Requirements/Responsibilities** An application processes data, giving it meaning. An application derives its sensitivity from the data it processes or contains. A computer derives its sensitivity from the applications it handles. Data owners determine sensitivity.

**Template Sections 1.4 and 2**

**Security Requirements**

- The data owner has identified authorized users and custodians.
- The data owner has identified and protected private data from unauthorized disclosure.
- The data owner has ensured that hard copy output (including electronic media) is controlled as necessary.
- The data owner has ensured implementation of file access controls as appropriate.
- The information category or sensitivity of the application/information is specified by the data owner.
- The security protections to be implemented have been specified by the data owner.

**Application Data Backup/Recovery:** Application data backup/recovery defines the owner's requirements to restore the application/information after a system malfunction or compromise of integrity.

**Template Section 10**

**Security Requirements**

- Backups of operating system releases are retained at least 3 generations or 1 year (whichever is longer.
- The most recent backup, or most recent minus one, is stored in a facility external to the site.
- The frequency of application data backups is defined.
- Data recovery procedures are defined and tested.

**Software Acceptance Testing:** COTS software is software that has been placed on the market as a saleable item. Software Acceptance Testing for IT security features provides a measure of assurance that the product correctly provides the advertised capabilities.

**Template Sections 1.4 and 5.3**

**Security Requirements**

- A test or inspection of available source code is performed to ensure that the program and installation scripts are free from malicious or unauthorized code.

- Function, reliability, and penetration tests are included in a test plan and performed.
- Testing and verification of security controls and application features are witnessed by appropriate personnel and documented.

**Maintenance of COTS Software:** COTS software maintenance (I.e. modifications and updates) increases the risk that errors, accidents, and intentional acts can occur.

**Template Sections 1.4 and 5.3**

**Security Requirements**

- All vendor-recommended application updates are reviewed, evaluated and tested to ensure they are free from malicious or unauthorized code.
- Software is controlled by a configuration management process.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.

**Template Sections 5.3 and 7**

**Security Requirements**

- All public domain mainframe software is approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.
- All solicited or unsolicited sample programs are approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.

**Template Section 1.4**

**Security Requirements**

- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.
- Operational security controls are reviewed and enforced.

**Encryption of Unclassified Data Requirement:** Encryption needs to be used on sensitive/critical data only if the risk analysis process for that system so dictates. When encryption is employed, the algorithm specified in FIPS 46-1 will be used in production systems.

**Template Sections 5.4 and 10**

**Security Requirements**

- A key management process is established and maintained.
- A data recovery process is maintained to ensure that information is accessible.

**Key Management:** Key management refers to the generation, distribution, storage, and destruction of keys used to encrypt and decrypt data.

**Template Section 5.4**

**Security Requirements**

- Electronically stored cryptographic keys are afforded the same level of security as the information they protect.
- A key owner for each cryptographic key is designated and recorded.
- The key owner distributes the cryptographic key to authorized personnel only.
- The cryptographic key is delivered to recipients in a manner that is at least as secure as logon password distribution.

**Password Encryption:** Passwords are encrypted if it is possible for either privileged or nonprivileged users to browse memory or disk storage where passwords are kept.

**Template Sections 5.7 and 10**

**Security Requirements**

- Password files on backup tapes are encrypted if it is possible for either privileged or nonprivileged users to browse the tapes.

**Private Data:** Private data is information which has disclosure restrictions such as Privacy Act, source selection, contractor proprietary, or medical data.

**Template Sections 5.4 and 10**

**Security Requirements**

- Private files on backup tapes are encrypted if the tape library system has no other mechanism for providing controlled access protection to the data.
- Private data is encrypted if the system has no other mechanism for providing controlled browse access protection to the data.

**Documentation:** Centralized operations refer to tasks that support multiuser systems, such as the operation and monitoring of console control units and peripherals, job scheduling, media retention and accountability, job quality control, etc.

**Template Section 5.5**

**Security Requirements**

- A list of personnel responsible for system and application software is maintained.
- Risk analysis, risk reduction, and contingency plans are developed and maintained.
- Applications are reviewed annually for changes in information categories/sensitivity level.
- A list of system security software problems is maintained and reviewed (as directed by management.)
- A complete inventory of system software and applications software is maintained.
- Complete operating system and appropriate application documentation is retained.
- Operating procedures and checklists are developed, used and maintained.

**Privileged Operations**

**Template Sections 5.5, 5.7, and 5.8**

**Security Requirements**

- Operator console logs are reviewed regularly.
- Only the operations group is authorized to disable console logging and that the event is logged when performed.
- Operators do not transfer privileged activity outside the operations area without proper authorization.

- Access to operator consoles is controlled.
- Both manual and automatic console logs are maintained and archived.
- IT security incidents are documented and reported to the Computer Security Official or POC and management.

**Console Logon**
**Template Sections 5.5, 5.7, and 5.8**
**Security Requirements**

- Operators do not transfer privileged activity outside the operations area without proper authorization.
- Only the operations group is authorized to disable console logging and that the event is logged when performed.
- IT security incidents are documented and reported to the Computer Security Official or POC and management.
- Both manual and automatic console logs are maintained and archived.
- Operator console logs are reviewed regularly.

**Media Storage**
**Template Sections 5.1, 5.3, and 10**
**Security Requirements**

- The media library is in an environmentally controlled area.
- Media is protected from theft, vandalism, and natural disasters.
- Media containing restricted access data is degaussed (erased)/overwritten before being returned to use or excessed.
- A visual means of identification (I.e., labels) is provided for all media containing private data.
- All media is identified with an external label and, when applicable, an internal label.
- A media inventory is maintained and verified at least semiannually.
- Only authorized personnel have access to the media.
- An inventory accounting system for all media entering or leaving a media storage facility is provided when appropriate.

**Job Input/Output**
**Template Section 5.2**
**Security Requirements**

- Input comes from an authorized source.
- The output is distributed only to authorized personnel.
- The appropriate cover sheet is attached to all output containing restricted access data.
- Only the minimum number of copies required to support the distribution are produced.
- All output for which there are disclosure restrictions, and which have not been distributed after a time period specified by management, is destroyed.

**Authentication Requirements:** Authentication is the process by which a computer verifies the identity of a user. The process generally consists of the computer prompting for a user ID and, at

minimum, a password.

**Template Section 5.7**

**Security Requirements**

- Network devices detect and close broken sessions.
- Unattended dial-in diagnostics that bypass normal authentication are prohibited.
- Dial-in connections and connections from public networks (such as the Internet) are accepted only via a boundary system.
- All output for which there are disclosure restrictions, and which have not been distributed after a time period specified by managed, is destroyed.

**File Transfer and Remote Logon Protection Requirements:** Services provided by the network include such processes as file transfer and remote logon.

**Template Sections 5.6 and 5.7**

**Security Requirements**

- Digital signatures or multiple checksums are employed to ensure the integrity of file transfer.
- Proxy or trusted logons are restricted.
- Only specifically authorized users are allowed to import software.
- Access to any privileged network software is restricted to a list of specifically authorized users.
- Inbound or outbound file transfer is prohibited from unauthenticated users (I.e., no anonymous file transfer).
- Inbound remote command execution is prohibited without user authentication.

**Connection Requirements:** Network attachment increases the number of threats to which a system may be vulnerable. Therefore, certain security precautions must be taken before a system is attached to a network.

**Template Section 5.3**

**Security Requirements**

- The risks associated with connecting to proposed network/nodes are determined to be acceptable.
- Trusted network partners (e.g., those the local system trusts to authenticate users) have implemented security protections equivalent to or acceptable to the local system.

**Additional Requirements for Boundary Systems:** Boundary systems are critical elements in providing a security perimeter for networks. The boundary system provides isolation and security services to the systems within the perimeter. Therefore, its own internal configuration must be maintained.

**Template Sections 5.6 and 5.7**

**Security Requirements**

- The boundary system will use extended user authentication to authenticate incoming user sessions destined for nodes inside the security perimeter.
- Only administrator and service accounts, but no user accounts, are supported on the boundary system.
- File transfer (ftp) and terminal emulation (telnet) sessions may be supported in both directions through the boundary system.

- Outbound user sessions may be supported with no extra authentication required.
- E-mail is supported only through a store-and-forward service on the boundary system.

## II. Multiuser Workstations

A multiuser workstation, also known as a host system, is one that can be accessed simultaneously by other workstations.

**Journaling and Monitoring:** Most multiuser computers have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or security problems.

**Template Section 5.8**
**Security Requirements**

- System journals record security-related events.
- Journals are reviewed daily or when problems are suspected.
- Successful and failed logons/logoffs are recorded.
- All file creation/modification/deletion events are recorded.
- Journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts.

**Individual Accountability**
**Template Section 7**
**Security Requirements**

- Individuals are held accountable for the protection against loss or disclosure of password they possess.
- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not equal to the user ID.
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.
- The password is not the name of a vendor product or a nickname for a product.
- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password expires after 30 days maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.
- Personal passwords are not shared.
- Group passwords are not allowed.

**Password Reuse**
**Template Sections 5.7 and 7**
**Security Requirements**

- The owner uses a minimum of 10 passwords before reuse.

**Password Storage**
**Template Section 5.7**
**Security Requirements**

- Stored passwords are protected in such a way that only the password system is authorized access to a password.
- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

**Password Distribution**
**Template Section 5.7**
**Security Requirements**

- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Passwords are not visible at the user terminal when being typed.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.
- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is reset by the user during the first sign-on.
- A new nontrivial password is assigned at the user's request.
- The policy ensures that positive identification of the user ID owner is provided.
- The policy ensures that the name, location, phone number, and system user ID of the

user needing reset is confirmed.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password is changed during the first logon by the user.
- The initial user password assignment is nontrivial.
- All vendor-supplied passwords are removed.

**User Authentication: Local Logon (used to log on directly to a system):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- User identification and local authentication (at least passwords) is required for all user ID's.

**User Authentication: Remote Logon (access a second system from the first without invoking a second authentication):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- Remote authentication is permitted at the discretion of the remote system admin when the authenticating system meets all security requirements of the remote system, audit trails are created, and the risk of subverting the connection is acceptable.

**Failed Logon Attempts:** Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination. Excessive failed logon attempts may indicate that an unauthorized user is attempting to access the system.
**Template Section 5.7 and 5.8**
**Security Requirements**

- The user ID owner is notified of failed logon attempts.
- The system notifies the System Administrator of user ID suspensions.
- The user ID is suspended, by system intervention, after three or fewer unsuccessful logon attempts or provides some form of system evasive action.
- The log of unsuccessful logon attempts is reviewed daily.

**Controlled Access Protection:** Controlled access protection is the ability of the system to control which users have access to resources. Ensure that all systems accessed will provide controlled access protection when users are not authorized for all information on the system.
**Template Sections 5.7 and 5.8**
**Security Requirements**

- The system provides audit trails or a journal of security-relevant events.

- The system provides individual electronic accountability through identification and authentication of each system user.
- The system provides the ability to control a user's access to information.

**Default File Protection:** Default file protection is the access control the system places on a file when the data owner does not take explicit action.

**Template Section 5.7**

**Security Requirements**

- System default file protection parameters are set to prevent read and execute access by anyone except the file owner and necessary operating system components.
- System default file protection parameters are set to grant write access to the file owner and to necessary operating system components.

**Data Owner Requirements/Responsibilities:** An application processes data, giving it meaning. An application derives its sensitivity from the data it processes or contains. A computer derives its sensitivity from the applications it handles. Data owners determine sensitivity.

**Template Sections 1.4 and 2**

**Security Requirements**

- The data owner has identified and protected private data from unauthorized disclosure.
- The information category or sensitivity of the application/information is specified by the data owner.
- The data owner has ensured that hard copy output (including electronic media) is controlled as necessary.
- The data owner has identified authorized users and custodians.
- The security protections to be implemented have been specified by the data owner.
- The data owner has ensured implementation of file access controls as appropriate.

**Application Data Backup/Recovery:** Application data backup/recovery defines the owner's requirements to restore the application/information after a system malfunction or compromise of integrity.

**Template Section 10**

**Security Requirements**

- Backups of operating system releases are retained at least 3 generations or 1 year (whichever is longer.
- Data recovery procedures are defined and tested.
- The most recent backup, or most recent minus one, is stored in a facility external to the site.
- The frequency of application data backups is defined.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.

**Template Sections 5.3 and 7**

**Security Requirements**

- All public domain workstation software is approved by an officially appointed staff

member who ensure that the software is free of malicious code before installation.
- All solicited or unsolicited sample programs are approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.

**Template Section 1.4**
**Security Requirements**
- Operational security controls are reviewed and enforced.
- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.

**Multiuser Workstations**
**Security Requirements**
- A system Administrator is assigned.
- Backup requirements are established.
- Virus detection software is installed in the workstation where applicable.
- System configuration is documented.
- A risk management program appropriate to the sensitivity level being processed is implemented.

## III. Singleuser Workstation

A single-user workstation is one that may be used by only one person at a time, though many people have access.

**Individual Accountability:**
**Template Section 7**
**Security Requirements**
- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.
- Individuals are held accountable for the protection against loss or disclosure of password they possess.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**
- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not the name of a vendor product or a nickname for a product.
- The password is not equal to the user ID.
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password expires after 30 days maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- Personal passwords are not shared.
- Group passwords are not allowed.
- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.

**Password Reuse**
**Template Sections 5.7 and 7**
**Security Requirements**

-The owner uses a minimum of 10 passwords before reuse.

**Password Storage**
**Template Section 5.7**
**Security Requirements**

- Stored passwords are protected in such a way that only the password system is authorized access to a password.
- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

**Password Distribution**
**Template Section 5.7**
**Security Requirements**

- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.
- Passwords are not visible at the user terminal when being typed.
- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.
- The policy ensures that positive identification of the user ID owner is provided.
- A new nontrivial password is assigned at the user's request.
- The password is reset by the user during the first sign-on.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password assignment is nontrivial.
- The initial user password is changed during the first logon by the user.
- All vendor-supplied passwords are removed.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.
**Template Sections 5.3 and 7**
**Security Requirements**

- All solicited or unsolicited sample programs are approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.
- All public domain workstation software is approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.
**Template Section 1.4**
**Security Requirements**

- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.
- Operational security controls are reviewed and enforced.

**Single User Workstations**
**Security Requirements**

- Virus detection software is installed on all applicable workstations.
- A risk management program commensurate with the information category/sensitivity level is implemented.
- Backup and recovery requirements are established.

## Baseline Security Requirements for Systems Rated Business and Restricted Technology (BRT)

## I. Servers and Mainframes

**Critical System Files Protection:** Critical system files are those that are integral to the operating system, system security mechanisms, or key system services. Corrupting these files would damage the integrity of the system.

**Template Section 5.7**

**Security Requirements**

- A list of authorized users of critical system files is maintained and verified at least semiannually.
- Configuration control is implemented for critical system files.
- Critical system file protection is reviewed at least semiannually.
- Access to password files is restricted to user ID management personnel.
- Access to critical system files are restricted to a minimum number of authorized system support personnel.
- Critical system files are identified and protected.
- File access is controlled.

**Privileged Users and Programs:** A privileged user is one who can alter or circumvent the operating system or the system's security privileges. A privileged program may have the capability to override or bypass security measures when executed. It is vital to monitor privileged access.

**Template Section 5.7**

**Security Requirements**

- Operating system privileges are assigned to a minimum number of systems personnel.
- System administration/support personnel do not function as system auditors.
- Access is controlled to privileged programs.
- A list of privileged users is maintained and verified at least semiannually.

**Journaling and Monitoring:** Most multiuser computers have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or security problems.

**Template Section 5.8**

**Security Requirements**

- Journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts.
- Critical system file modification or modification attempts are recorded.
- All successful and failed file opens and closes are recorded, at the discretion of the manager.
- The system journals record security-related events, unless specifically waived by the functional manager of the application software.
- Successful and failed logons/logoffs are recorded.
- Journals are reviewed weekly, or more frequently when problems are suspected.

**System Retention/Backup:** To ensure continuity of operation, copies of important software and data will be made and retained.

**Template Section 10**

**Security Requirements**

- Operating systems and key system services are backed up at least monthly and when modified.
- Monthly operating system backups are retained for at least 6 months.
- Journals are retained for at least 6b months.
- The most recent, or most recent minus one, backup is stored external to the site.

**System Shutdown/Restart:** The system should provide security safeguards to cover unscheduled system shutdowns, (e.g., aborts) and subsequent restarts as well as for scheduled shutdowns and startups.

**Template Section 5.8**

**Security Requirements**

- All aborts and restarts are logged and documented.
- Only authorized personnel shutdown/restart the system.
- System shutdown/restart procedures are documented.

**Operating System Local Modifications:** Local modifications to the operating system can have security implications. If incorrectly designed or implemented, local operating systems modifications may invalidate the system's security controls.

**Template Section 5.3**

**Security Requirements**

- All operating system security modifications are reviewed and approved.
- All operating system modifications are tested and/or evaluated for impact on security before permanent installation.
- All operating system security modifications are documented.

**Configuration Management:** Because the operating system governs the security of the system, changes to the operating system, including new releases and updates, will be controlled and monitored.

**Template Section 5.3**

**Security Requirements**

- All operating system changes are tested and/or evaluated and documented.
- Change control for critical system files is documented.

**User ID Approval Process/Privileges:** A process must be put in place to ensure that all requests for user ID's are reviewed and approved by management. A list of personnel who are authorized to approve the user ID's will be furnished to the appropriate user-ID administrator.

**Template Sections 7 and 9**

**Security Requirements**

- Group user ID's are restricted to the minimum number necessary to conduct system operations.
- Personnel screening and IT security briefing is verified.

- All individuals assigned a user ID sign a statement of responsibility indicating their understanding for using and safeguarding the information to which he/she is granted access.
- The statement of responsibility is retained by user ID management for every active account.
- The user ID is removed after 180 days if the password has not been changed after notification
- The user ID is suspended after 90 days if the password has not been changed after notification
- Each employee submits a formal request to the appropriate administrator for a user ID, which indicates the category being requested, such as group, personal, privileged, project, application system service, or generic.
- The request for a user ID is approved by the employee's manager. (If the employee is a contractor or other non-NASA employee, the approval of the employee's NASA sponsor is also required.)

**Group User ID's:** Group user ID's are discouraged because individual accountability is lost. However, if the system is configured such that group user ID's must be used, approval processes must be put in place.

**Template Section 5.6**
**Security Requirements**

- Group user ID's are not provided without risk justification and concurrence from all functional mangers of the affected data and applications.

**User ID Revalidation:** Management will ensure that an inventory is maintained of all assigned user ID's.

**Template Section 5.6**
**Security Requirements**

- All group user ID's are revalidated at least annually.
- A statement of responsibility is on file for each person who has a group user ID.

**Disposition of Unused User ID's:** Management will ensure that proper disposition is made of all unused user ID's. User ID disposition uses password lifetime as the metric for user-ID-deletion decisions.

**Template Section 5.6**
**Security Requirements**

- A user will be reminded to change his or her password for 30 days.

**User ID Reuse:** User ID's may be reassigned after removal from the system under the following condition(s).

**Template Section 5.6**
**Security Requirements**

- A user ID may be reassigned after all access rights and privileges associated with the user ID have been removed.

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual is terminated for **cause of because of reduction in force.**

**Template Section 5.6**

**Security Requirements**

- The user ID is removed as soon as practical, but no later than the end of the day of termination.

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual has **resigned, received a change of job, or has retired**, and no longer requires access to the system to perform assigned duties.

**Template Section 5.6**

**Security Requirements**

- The user ID is removed within 5 working days.

**Individual Accountability**

**Template Section 7**

**Security Requirements**

- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.
- Individuals are held accountable for the protection against loss or disclosure of password they possess.

**Password Length and Composition**

**Template Sections 5.7 and 7**

**Security Requirements**

- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.
- Passwords have a minimum of eight characters.

**Password Triviality**

**Template Sections 5.7 and 7**

**Security Requirements**

- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.
- The password is not the name of a vendor product or a nickname for a product.
- The password is not equal to the user ID.

**Password Maximum Lifetime**

**Template Sections 5.7 and 7**

**Security Requirements**

- The password expires after 90 days maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant temporary access to another individual.
- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.

**Password Reuse**
**Template Sections 5.7 and 7**
**Security Requirements**

- The owner uses a minimum of 10 passwords before reuse.

**Password Storage**
**Template Section 5.7**
**Security Requirements**

- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).
- Stored passwords are protected in such a way that only the password system is authorized access to a password.

**Password Distribution**
**Template Section 5.7**
**Security Requirements**

- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Passwords are not visible at the user terminal when being typed.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.
- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is reset by the user during the first sign-on.
- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.
- The policy ensures that positive identification of the user ID owner is provided.
- A new nontrivial password is assigned at the user's request.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password is changed during the first logon by the user.
- The initial user password assignment is nontrivial.
- All vendor-supplied passwords are removed.

**User Authentication: Local Logon (used to log on directly to a system) :** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).

**Template Section 5.7**

**Security Requirements**

- User identification and local authentication (at least passwords) is required for all user ID's.

**User Authentication: Remote Logon (access a second system from the first without invoking a second authentication):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).

**Template Section 5.7**

**Security Requirements**

- Remote authentication is permitted at the discretion of the remote system admin when the authenticating system meets all security requirements of the remote system, audit trails are created, and the risk of subverting the connection is acceptable.

**Failed Logon Attempts:** Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination. Excessive failed logon attempts may indicate that an unauthorized user is attempting to access the system.

**Template Section 5.7 and 5.8**

**Security Requirements**

- The log of unsuccessful logon attempts is reviewed weekly.
- The user ID is suspended, by system intervention, after five or fewer unsuccessful logon attempts or provides some form of system evasive action.
- The user ID owner is notified of failed logon attempts.
- The system notifies the System Administrator of user ID suspensions.

**Controlled Access Protection:** Controlled access protection is the ability of the system to control which users have access to resources. Ensure that all systems accessed will provide controlled access protection when users are not authorized for all information on the system.

**Template Sections 5.7 and 5.8**

**Security Requirements**

- The system provides audit trails or a journal of security-relevant events.
- The system provides the ability to control a user's access to information.
- The system provides individual electronic accountability through identification and authentication of each system user.

**Default File Protection:** Default file protection is the access control the system places on a file when the data owner does not take explicit action.

**Template Section 5.7**

**Security Requirements**

- System default file protection parameters are set to grant write access to the file owner and to necessary operating system components.
- System default file protection parameters are set to prevent read and execute access by anyone except the file owner and necessary operating system components.

**Data Owner Requirements/Responsibilities:** An application processes data, giving it meaning. An application derives its sensitivity from the data it processes or contains. A computer derives its sensitivity from the applications it handles. Data owners determine sensitivity.

**Template Sections 1.4 and 2**

**Security Requirements**

- The data owner has identified authorized users and custodians.
- The data owner has identified and protected private data from unauthorized disclosure.
- The data owner has ensured that hard copy output (including electronic media) is controlled as necessary.
- The data owner has ensured implementation of file access controls as appropriate.
- The security protections to be implemented have been specified by the data owner.
- The information category or sensitivity of the application/information is specified by the data owner.

**Application Data Backup/Recovery:** Application data backup/recovery defines the owner's requirements to restore the application/information after a system malfunction or compromise of integrity.

**Template Section 10**

**Security Requirements**

- The frequency of application data backups is defined.
- Data recovery procedures are defined and tested.
- At least three generations of backups are retained.
- The most recent backup, or most recent minus one, is stored in an external facility.

**Software Acceptance Testing:** COTS software is software that has been placed on the market as a saleable item. Software Acceptance Testing for IT security features provides a measure of assurance that the product correctly provides the advertised capabilities.

**Template Sections 1.4 and 5.3**

**Security Requirements**

- A test or inspection of available source code is performed to ensure that the program and installation scripts are free from malicious or unauthorized code.
- Function, reliability, and penetration tests are included in a test plan and performed.
- Testing and verification of security controls and application features are witnessed by appropriate personnel and documented.

**Maintenance of COTS Software:** COTS software maintenance (I.e. modifications and updates) increases the risk that errors, accidents, and intentional acts can occur.

**Template Sections 1.4 and 5.3**

**Security Requirements**

- All vendor-recommended application updates are reviewed, evaluated and tested to ensure they are free from malicious or unauthorized code.
- Software is controlled by a configuration management process.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.

**Template Sections 5.3 and 7**

**Security Requirements**

- All public domain mainframe software is approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.
- All solicited or unsolicited sample programs are approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.

**Template Section 1.4**

**Security Requirements**

- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.
- Operational security controls are reviewed and enforced.

**Encryption of Unclassified Data Requirement:** Encryption needs to be used on sensitive/critical data only if the risk analysis process for that system so dictates. When encryption is employed, the algorithm specified in FIPS 46-1 will be used in production systems.

**Template Sections 5.4 and 10**

**Security Requirements**

- A key management process is established and maintained.
- A data recovery process is maintained to ensure that information is accessible.

**Key Management:** Key management refers to the generation, distribution, storage, and destruction of keys used to encrypt and decrypt data.

**Template Section 5.4**

**Security Requirements**

- A key owner for each cryptographic key is designated and recorded.
- The key owner distributes the cryptographic key to authorized personnel only.
- The cryptographic key is delivered to recipients in a manner that is at least as secure as logon password distribution.
- Electronically stored cryptographic keys are afforded the same level of security as

the information they protect.

**Password Encryption**
**Template Sections 5.7 and 10**
**Security Requirements**

- Passwords are encrypted if it is possible for either privileged or nonprivileged users to browse memory or disk storage where passwords are kept.
- Password files on backup tapes are encrypted if it is possible for either privileged or nonprivileged users to browse the tapes.

**Private Data:** Private data is information which has disclosure restrictions such as Privacy Act, source selection, contractor proprietary, or medical data.
**Template Sections 5.4 and 10**
**Security Requirements**

- Private data is encrypted if the system has no other mechanism for providing controlled browse access protection to the data.
- Private files on backup tapes are encrypted if the tape library system has no other mechanism for providing controlled access protection to the data.

**Documentation:** Celized operations refer to tasks that support multiuser systems, such as the operation and monitoring of console control units and peripherals, job scheduling, media retention and accountability, job quality control, etc.
**Template Section 5.5**
**Security Requirements**

- Complete operating system and appropriate application documentation is retained.
- A list of personnel responsible for system and application software is maintained.
- Risk analysis, risk reduction, and contingency plans are developed and maintained.
- Applications are reviewed annually for changes in information categories/sensitivity level.
- A list of system security software problems is maintained and reviewed (as directed by management.)
- Operating procedures and checklists are developed, used and maintained.
- A complete inventory of system software and applications software is maintained.

**Privileged Operations**
**Template Sections 5.5, 5.7, and 5.8**
**Security Requirements**

- Operator console logs are reviewed regularly.
- Operators do not transfer privileged activity outside the operations area without proper authorization.
- Both manual and automatic console logs are maintained and archived.
- Access to operator consoles is controlled.
- IT security incidents are documented and reported to the Computer Security Official or POC and management.
- Only the operations group is authorized to disable console logging and that the event is logged when performed.

**Console Logon**
**Template Sections 5.5, 5.7, and 5.8**
**Security Requirements**

- Operators do not transfer privileged activity outside the operations area without proper authorization.
- Only the operations group is authorized to disable console logging and that the event is logged when performed.
- IT security incidents are documented and reported to the Computer Security Official or POC and management.
- Both manual and automatic console logs are maintained and archived.
- Operator console logs are reviewed regularly.

**Media Storage**
**Template Sections 5.1, 5.3, and 10**
**Security Requirements**

- Only authorized personnel have access to the media.
- Media is protected from theft, vandalism, and natural disasters.
- Media containing restricted access data is degaussed (erased)/overwritten before being returned to use or excessed.
- A visual means of identification (I.e., labels) is provided for all media containing private data.
- All media is identified with an external label and, when applicable, an internal label.
- An inventory accounting system for all media entering or leaving a media storage facility is provided when appropriate.
- The media library is in an environmentally controlled area.
- A media inventory is maintained and verified at least semiannually.

**Job Input/Output**
**Template Section 5.2**
**Security Requirements**

- Input comes from an authorized source.
- Restricted access output is distributed only to authorized personnel.
- The appropriate cover sheet is attached to all output containing restricted access data.
- Any restricted access data which has not been distributed after a time period specified by management, is destroyed.

**Authentication Requirements:** Authentication is the process by which a computer verifies the identity of a user. The process generally consists of the computer prompting for a user ID and, at minimum, a password. Unattended dial-in diagnostics that bypass normal authentication are prohibited.
**Template Section 5.7**
**Security Requirements**

- Dial-in connections and connections from public networks (such as the Internet) are

accepted only via a boundary system.
- All output for which there are disclosure restrictions, and which have not been distributed after a time period specified by managed, is destroyed.
- Network devices detect and close broken sessions.

**File Transfer and Remote Logon Protection Requirement:** Services provided by the network include such processes as file transfer and remote logon.

**Template Sections 5.6 and 5.7**

**Security Requirements**

- Digital signatures or multiple checksums are employed to ensure the integrity of file transfer.
- Proxy or trusted logons are restricted.
- Only specifically authorized users are allowed to import software.
- Access to any privileged network software is restricted to a list of specifically authorized users.
- Inbound or outbound file transfer is prohibited from unauthenticated users (I.e., no anonymous file transfer).
- Inbound remote command execution is prohibited without user authentication.

**Connection Requirements:** Network attachment increases the number of threats to which a system may be ulnerable. Therefore, certain security precautions must be taken before a system is attached to a network.

**Template Section 5.3**

**Security Requirements**

- The risks associated with connecting to proposed network/nodes are determined to be acceptable.
- Trusted network partners (e.g., those the local system trusts to authenticate users) have implemented security protections equivalent to or acceptable to the local system.

**Additional Requirements for Boundary Systems:** Boundary systems are critical elements in providing a security perimeter for networks. The boundary system provides isolation and security services to the systems within the perimeter. Therefore, its own internal configuration must be maintained.

**Template Sections 5.6 and 5.7**

**Security Requirements**

- The boundary system will use extended user authentication to authenticate incoming user sessions destined for nodes inside the security perimeter.
- Only administrator and service accounts, but no user accounts, are supported on the boundary system.
- File transfer (ftp) and terminal emulation (telnet) sessions may be supported in both directions through the boundary system.
- Outbound user sessions may be supported with no extra authentication required.
- E-mail is supported only through a store-and-forward service on the boundary system.

## II. Multiuser Workstations

A multiuser workstation, also known as a host system, is one that can be accessed

simultaneously by other workstations.

**Journaling and Monitoring:** Most multiuser computers have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or security problems.

**Template Section 5.8**
**Security Requirements**

- Successful and failed logons/logoffs are recorded.
- Journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts.
- The system journals record security-related events, unless specifically waived by the functional manager of the application software.
- Journals are reviewed weekly, or more frequently when problems are suspected.
- All successful and failed file opens and closes are recorded, at the discretion of the manager.
- Critical system file modification or modification attempts are recorded.

**Individual Accountability**
**Template Section 7**
**Security Requirements**

- Individuals are held accountable for the protection against loss or disclosure of password they possess.
- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not the name of a vendor product or a nickname for a product.
- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not equal to the user ID.
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password expires after 90 days maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.
- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant temporary access to another individual.

**Password Reuse**
**Template Sections 5.7 and 7**
**Security Requirements**

- The owner uses a minimum of 10 passwords before reuse.

**Password Storage**
**Template Section 5.7**
**Security Requirements**

- Stored passwords are protected in such a way that only the password system is authorized access to a password.
- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

**Password Distribution**
**Template Section 5.7**
**Security Requirements**

- Passwords are not visible at the user terminal when being typed.
- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.
- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is reset by the user during the first sign-on.
- A new nontrivial password is assigned at the user's request.
- The policy ensures that positive identification of the user ID owner is provided.
- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password is changed during the first logon by the user.
- The initial user password assignment is nontrivial.
- All vendor-supplied passwords are removed.

**User Authentication: Local Logon (used to log on directly to a system) :** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- User identification and local authentication (at least passwords) is required for all user ID's.

**User Authentication: Remote Logon (access a second system from the first without invoking a second authentication):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- Remote authentication is permitted at the discretion of the remote system admin when the authenticating system meets all security requirements of the remote system, audit trails are created, and the risk of subverting the connection is acceptable.

**Failed Logon Attempts:** Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination. Excessive failed logon attempts may indicate that an unauthorized user is attempting to access the system.
**Template Section 5.7 and 5.8**
**Security Requirements**

- The log of unsuccessful logon attempts is reviewed weekly.
- The user ID owner is notified of failed logon attempts.
- The system notifies the System Administrator of user ID suspensions.
- The user ID is suspended, by system intervention, after five or fewer unsuccessful logon attempts or provides some form of system evasive action.

**Controlled Access Protection:** Controlled access protection is the ability of the system to control which users have access to resources. Ensure that all systems accessed will provide controlled access protection when users are not authorized for all information on the system.
**Template Sections 5.7 and 5.8**
**Security Requirements**

- The system provides audit trails or a journal of security-relevant events.
- The system provides individual electronic accountability through identification and authentication of each system user.

- The system provides the ability to control a user's access to information.

**Default File Protection:** Default file protection is the access control the system places on a file when the data owner does not take explicit action.

**Template Section 5.7**

**Security Requirements**

- System default file protection parameters are set to prevent read and execute access by anyone except the file owner and necessary operating system components.
- System default file protection parameters are set to grant write access to the file owner and to necessary operating system components.

**Data Owner Requirements/Responsibilities:** An application processes data, giving it meaning. An application derives its sensitivity from the data it processes or contains. A computer derives its sensitivity from the applications it handles. Data owners determine sensitivity.

**Template Sections 1.4 and 2**

**Security Requirements**

- The data owner has identified and protected private data from unauthorized disclosure.
- The information category or sensitivity of the application/information is specified by the data owner.
- The data owner has ensured that hard copy output (including electronic media) is controlled as necessary.
- The data owner has identified authorized users and custodians.
- The security protections to be implemented have been specified by the data owner.
- The data owner has ensured implementation of file access controls as appropriate.

**Application Data Backup/Recovery:** Application data backup/recovery defines the owner's requirements to restore the application/information after a system malfunction or compromise of integrity.

**Template Section 10**

**Security Requirements**

- The frequency of application data backups is defined.
- The most recent backup, or most recent minus one, is stored in an external facility.
- Data recovery procedures are defined and tested.
- At least three generations of backups are retained.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.

**Template Sections 5.3 and 7**

**Security Requirements**

- All public domain workstation software is approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.
- All solicited or unsolicited sample programs are approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.

**Template Section 1.4**

**Security Requirements**

- Operational security controls are reviewed and enforced.
- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.

**Multiuser Workstations**

**Security Requirements**

- Critical data backups are placed in secure storage.
- Secure backup storage is provided external to the processing area.
- Each user is identified by a unique user ID and password.
- A System Administrator is assigned.
- Backup requirements are established.
- Virus detection software is installed in the workstation where applicable.
- System configuration is documented.
- A risk management program appropriate to the sensitivity level being processed is implemented.

## III. Singleuser Workstation

A single-user workstation is one that may be used by only one person at a time, though many people have access.

**Individual Accountability**

**Template Section 7**

**Security Requirements**

- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.
- Individuals are held accountable for the protection against loss or disclosure of password they possess.

**Password Length and Composition**

**Template Sections 5.7 and 7**

**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**

**Template Sections 5.7 and 7**

**Security Requirements**

- The password is not either wholly or predominantly composed of personal information

(family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not the name of a vendor product or a nickname for a product.
- The password is not equal to the user ID.
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**
- The password expires after 90 days maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**
- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant temporary access to another individual.
- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.

**Password Reuse**
**Template Sections 5.7 and 7**
**Security Requirements**
- The owner uses a minimum of 10 passwords before reuse.

**Password Storage**
**Template Section 5.7**
**Security Requirements**
- Stored passwords are protected in such a way that only the password system is authorized access to a password.
- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

**Password Distribution**
**Template Section 5.7**
**Security Requirements**
- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.
- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.
- Passwords are not visible at the user terminal when being typed.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.
- The policy ensures that positive identification of the user ID owner is provided.
- A new nontrivial password is assigned at the user's request.
- The password is reset by the user during the first sign-on.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password assignment is nontrivial.
- The initial user password is changed during the first logon by the user.
- All vendor-supplied passwords are removed.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.
**Template Sections 5.3 and 7**
**Security Requirements**

- All solicited or unsolicited sample programs are approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.
- All public domain workstation software is approved by an officially appointed staff member who ensure that the software is free of malicious code before installation.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.
**Template Section 1.4**
**Security Requirements**

- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.
- Operational security controls are reviewed and enforced.

**Single User Workstations**
**Security Requirements**

- Virus detection software is installed on all applicable workstations.
- A risk management program commensurate with the information category/sensitivity level is implemented.
- Backup and recovery requirements are established.

## Baseline Security Requirements for Systems Rated Scientific, Engineering, and Research (SER) or Administrative (ADM)

## I. Servers and Mainframes

**Critical System Files Protection:** Critical system files are those that are integral to the operating system, system security mechanisms, or key system services. Corrupting these files would damage the integrity of the system.

**Template Section 5.7**

**Security Requirements**

- Access to password files is restricted.
- Critical system file protection is reviewed at least annually.
- Access to critical system files is restricted to authorized users.
- Critical system files are identified and protected.
- File access is controlled.

**Privileged Users and Programs:** A privileged user is one who can alter or circumvent the operating system or the system's security privileges. A privileged program may have the capability to override or bypass security measures when executed. It is vital to monitor privileged access.

**Template Section 5.7**

**Security Requirements**

- Operating system privileges are assigned to a minimum number of systems personnel.

**Journaling and Monitoring:** Most multiuser computers have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or ecurity problems.

**Template Section 5.8**

**Security Requirements**

- Successful and failed logons/logoffs are recorded.
- Critical system file modifications are recorded.
- Journals are reviewed monthly, or more frequently when problems are suspected.
- System journals record security-relevant events as directed by management.
- Journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts.

**System Retention/Backup:** To ensure continuity of operation, copies of important software and data will be made and retained.

**Template Section 10**

**Security Requirements**

- Journals and system backups are retained as directed by the manager.

**System Shutdown/Restart:** The system should provide security safeguards to cover unscheduled system shutdowns, (e.g., aborts) and subsequent restarts as well as for scheduled shutdowns and startups.

**Template Section 5.8**

**Security Requirements**

- System shutdown/restart procedures are documented.
- Only authorized personnel restart the system.

**Operating System Local Modifications:** Local modifications to the operating system can have security implications. If incorrectly designed or implemented, local operating systems modifications may invalidate the system's security controls.

**Template Section 5.3**

**Security Requirements**

- Operating system security modifications are documented as directed by the manager.

**Configuration Management:** Because the operating system governs the security of the system, changes to the operating system, including new releases and updates, will be controlled and monitored.

**Template Section 5.3**

**Security Requirements**

- All operating system changes are tested and documented as directed by the manager.

**User ID Approval Process/Privileges:** A process must be put in place to ensure that all requests for user ID's are reviewed and approved by management. A list of personnel who are authorized to approve the user ID's will be furnished to the appropriate user-ID administrator.

**Template Sections 7 and 9**

**Security Requirements**

- Group user ID's are restricted to the minimum number necessary to conduct system operations.
- The user ID is removed after 240 days if the password has not been changed after notification
- The user ID is suspended after 120 days if the password has not been changed after notification
- All individuals requesting a user ID complete the appropriate request form, and sign a statement of responsibility indicating their understanding for using and safeguarding the information to which he/she is granted access.
- The statement of responsibility is retained by user ID management for a minimum of 1 year.

**User ID Revalidation:** Management will ensure that an inventory is maintained of all assigned user ID's.

**Template Section 5.6**

**Security Requirements**

- A statement of responsibility is on file for each person who has a group user ID.
- All group user ID's are revalidated at least annually.

**Disposition of Unused User ID's:** Management will ensure that proper disposition is made of all unused user ID's. User ID disposition uses password lifetime as the metric for user-ID-deletion decisions.

**Template Section 5.6**
**Security Requirements**

- A user will be reminded to change his or her password for 30 days.

**User ID Reuse:** User ID's may be reassigned after removal from the system under the following condition(s).

**Template Section 5.6**
**Security Requirements**

- A user ID may be reassigned in accordance with directives by the manager.

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual is terminated for **cause of because of reduction in force.**

**Template Section 5.6**
**Security Requirements**

- The user ID is removed within 2 working days of the termination.

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual has **resigned, received a change of job, or has retired,** and no longer requires access to the system to perform assigned duties.

**Template Section 5.6**
**Security Requirements**

- The user ID is removed within 15 working days.

**Individual Accountability**
**Template Section 7**
**Security Requirements**

- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.
- Individuals are held accountable for the protection against loss or disclosure of password they possess.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**

- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.
- Passwords have a minimum of eight characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not a word found in a dictionary of any language or a dictionary word

with numbers appended or prepended to it.
- The password is not equal to the user ID.
- The password is not the name of a vendor product or a nickname for a product.

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**
- The password expires after 1 year maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**
- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.
- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant ongoing access to another individual or may create a temporary password.

**Password Storage**
**Template Section 5.7**
**Security Requirements**
- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).
- Stored passwords are protected in such a way that only the password system is authorized access to a password.

**Password Distribution**
**Template Section 5.7**
**Security Requirements**
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.
- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.
- Passwords are not visible at the user terminal when being typed.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**
- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.
- The password is reset by the user during the first sign-on.
- A new nontrivial password is assigned at the user's request.
- The policy ensures that positive identification of the user ID owner is provided.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- All vendor-supplied passwords are removed.
- The initial user password assignment is nontrivial.
- The initial user password is changed during the first logon by the user.

**User Authentication: Local Logon (used to log on directly to a system):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- User identification and local authentication (at least passwords) is required for all user ID's.

**User Authentication: Remote Logon (access a second system from the first without invoking a second authentication):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**

- Remote authentication is permitted at the discretion of the remote system admin when the authenticating system meets all security requirements of the remote system, audit trails are created, and the risk of subverting the connection is acceptable.

**Failed Logon Attempts:** Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination. Excessive failed logon attempts may indicate that an unauthorized user is attempting to access the system.
**Template Section 5.7 and 5.8**
**Security Requirements**

- The user ID owner is notified of failed logon attempts.
- The user ID is suspended, by system intervention, after five or fewer unsuccessful logon attempts or provides some form of system evasive action.
- The log of unsuccessful logon attempts is reviewed weekly.

**Controlled Access Protection:** Controlled access protection is the ability of the system to control which users have access to resources. Ensure that all systems accessed will provide controlled access protection when users are not authorized for all information on the system.
**Template Sections 5.7 and 5.8**
**Security Requirements**

- The system provides audit trails or a journal of security-relevant events.
- The system provides individual electronic accountability through identification and authentication of each system user.

- The system provides the ability to control a user's access to information.

**Default File Protection:** Default file protection is the access control the system places on a file when the data owner does not take explicit action.

**Template Section 5.7**

**Security Requirements**

- System default file protection parameters are set to grant write and execute access to the file owner and to necessary operating system components.

**Data Owner Requirements/Responsibilities:** An application processes data, giving it meaning. An application derives its sensitivity from the data it processes or contains. A computer derives its sensitivity from the applications it handles. Data owners determine sensitivity.

**Template Sections 1.4 and 2**

**Security Requirements**

- The data owner has identified and protected private data from unauthorized disclosure.
- The information category or sensitivity of the application/information is specified by the data owner.
- The security protections to be implemented have been specified by the data owner.
- The data owner has identified authorized users and custodians.

**Software Acceptance Testing:** COTS software is software that has been placed on the market as a saleable item. Software Acceptance Testing for IT security features provides a measure of assurance that the product correctly provides the advertised capabilities.

**Template Sections 1.4 and 5.3**

**Security Requirements**

- Tests are performed that show the program is free from malicious or unauthorized code (e.g., scanning for known viruses, backdoors, logic bombs, and Trojan code).

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.

**Template Sections 5.3 and 7**

**Security Requirements**

- All mainframe public domain software not acquired through the normal procurement processes will be approved before installation in accordance with established requirements.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.

**Template Section 1.4**

**Security Requirements**

- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition,

design, programming and testing.
- Operational security controls are reviewed and enforced.

**Encryption of Unclassified Data Requirement:** Encryption needs to be used on sensitive/critical data only if the risk analysis process for that system so dictates. When encryption is employed, the algorithm specified in FIPS 46-1 will be used in production systems.
**Template Sections 5.4 and 10**
**Security Requirements**
- A key management process is established and maintained.
- A data recovery process is maintained to ensure that information is accessible.

**Key Management:** Key management refers to the generation, distribution, storage, and destruction of keys used to encrypt and decrypt data.
**Template Section 5.4**
**Security Requirements**
- A key owner for each cryptographic key is designated and recorded.
- The key owner distributes the cryptographic key to authorized personnel only.
- Electronically stored cryptographic keys are afforded the same level of security as the information they protect.
- The cryptographic key is delivered to recipients in a manner that is at least as secure as logon password distribution.

**Password Encryption**
**Template Sections 5.4, 5.7, and 10**
**Security Requirements**
- Passwords are encrypted if it is possible for either privileged or nonprivileged users to browse memory or disk storage where passwords are kept.
- Password files on backup tables are encrypted if it is possible for either privileged or nonprivileged users to browse the tapes.

**Private Data:** Private data is information which has disclosure restrictions such as Privacy Act, source selection, contractor proprietary, or medical data.
**Template Sections 5.4 and 10**
**Security Requirements**
- Private data is encrypted if the system has no other mechanism for providing controlled browse access protection to the data.
- Private files on backup tapes are encrypted if the tape library system has no other mechanism for providing controlled access protection to the data.

**Documentation:** Centralized operations refer to tasks that support multiuser systems, such as the operation and monitoring of console control units and peripherals, job scheduling, media retention and accountability, job quality control, etc.
**Template Section 5.5**
**Security Requirements**
- A list of personnel responsible for system and application software is maintained.
- A complete list of systems' applications is maintained.

- Complete operating system documentation is retained.
- Risk analysis, risk reduction, and contingency plans are developed and maintained.
- Applications are reviewed annually for changes in information categories/sensitivity level.
- Operating procedures and checklists are developed, used and maintained.
- A list of system security software problems is maintained and reviewed (as directed by management.)

**Privileged Operations**
**Template Sections 5.5, 5.7, and 5.8**
**Security Requirements**

- Access to operator consoles is controlled.
- Operators do not transfer privileged activity outside the operations area without proper authorization.
- Only the operations group is authorized to disable console logging and that the event is logged when performed.
- IT security incidents are documented and reported to the Computer Security Official or POC and management.
- Both manual and automatic console logs are maintained and archived.
- Operator console logs are reviewed regularly.

**Console Logon**
**Template Sections 5.5, 5.7, and 5.8**
**Security Requirements**

- Operators do not transfer privileged activity outside the operations area without proper authorization.
- Operator console logs are reviewed regularly.
- Only the operations group is authorized to disable console logging and that the event is logged when performed.
- IT security incidents are documented and reported to the Computer Security Official or POC and management.
- Both manual and automatic console logs are maintained and archived.

**Media Storage**
**Template Sections 5.1, 5.3, and 10**
**Security Requirements**

- The media library is in an environmentally controlled area.
- Only authorized personnel have access to the media.
- Media containing restricted access data is degaussed (erased)/overwritten before being returned to use or excessed.
- Media is protected from theft, vandalism, and natural disasters.

**Job Input/Output**
**Template Section 5.2**
**Security Requirements**

- Input comes from an authorized source.

- The appropriate cover sheet is attached to all output containing restricted access data.
- Restricted access output is distributed only to authorized personnel.
- Any restricted access data which has not been distributed after a time period specified by management, is destroyed.

**Authentication Requirements:** Authentication is the process by which a computer verifies the identity of a user. The process generally consists of the computer prompting for a user ID and, at minimum, a password.

**Template Section 5.7**

**Security Requirements**

- Network devices detect and close broken sessions.
- Unattended dial-in diagnostics that bypass normal authentication are prohibited.
- Dial-in connections and connections from public networks (such as the Internet) are accepted only via a boundary system.
- All output for which there are disclosure restrictions, and which have not been distributed after a time period specified by managed, is destroyed.

**File Transfer and Remote Logon Protection Requirements:** Services provided by the network include such processes as file transfer and remote logon.

**Template Sections 5.6 and 5.7**

**Security Requirements**

- Proxy or trusted logons are restricted.
- Inbound remote command execution is prohibited without user authentication.
- Digital signatures or multiple checksums are employed to ensure the integrity of file transfer.
- Only specifically authorized users are allowed to import software.
- Inbound or outbound file transfer is prohibited from unauthenticated users (I.e., no anonymous file transfer).
- Access to any privileged network software is restricted to a list of specifically authorized users.

**Connection Requirements:** Network attachment increases the number of threats to which a system may be vulnerable. Therefore, certain security precautions must be taken before a system is attached to a network.

**Template Section 5.3**

**Security Requirements**

- The risks associated with connecting to proposed network/nodes are determined to be acceptable.
- Trusted network partners (e.g., those the local system trusts to authenticate users) have implemented security protections equivalent to or acceptable to the local system.

**Additional Requirements for Boundary Systems:** Boundary systems are critical elements in providing a security perimeter for networks. The boundary system provides isolation and security services to the systems within the perimeter. Therefore, its own internal configuration must be maintained.

**Template Sections 5.6 and 5.7**
**Security Requirements**

- The boundary system will use extended user authentication to authenticate incoming user sessions destined for nodes inside the security perimeter.
- Only administrator and service accounts, but no user accounts, are supported on the boundary system.
- File transfer (ftp) and terminal emulation (telnet) sessions may be supported in both directions through the boundary system.
- Outbound user sessions may be supported with no extra authentication required.
- E-mail is supported only through a store-and-forward service on the boundary system.

## II. Multiuser Workstations

A multiuser workstation, also known as a host system, is one that can be accessed simultaneously by other workstations.

**Journaling and Monitoring:** Most multiuser computers have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or security problems.

**Template Section 5.8**
**Security Requirements**

- Successful and failed logons/logoffs are recorded.
- Journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts.
- System journals record security-relevant events as directed by management.
- Journals are reviewed monthly, or more frequently when problems are suspected.
- Critical system file modifications are recorded.

**Individual Accountability**
**Template Section 7**
**Security Requirements**

- Individuals are held accountable for the protection against loss or disclosure of password they possess.
- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not equal to the user ID.

- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.
- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not the name of a vendor product or a nickname for a product.

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password expires after 1 year maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.
- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant ongoing access to another individual or may create a temporary password.

**Password Storage**
**Template Section 5.7**
**Security Requirements**

- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).
- Stored passwords are protected in such a way that only the password system is authorized access to a password.

**Password Distribution**
**Template Section 5.7**
**Security Requirements**

- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Passwords are not visible at the user terminal when being typed.
- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The policy ensures that positive identification of the user ID owner is provided.
- The policy ensures that the name, location, phone number, and system user ID of the

user needing reset is confirmed.
- The password is reset by the user during the first sign-on.
- A new nontrivial password is assigned at the user's request.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**
- All vendor-supplied passwords are removed.
- The initial user password assignment is nontrivial.
- The initial user password is changed during the first logon by the user.

**User Authentication: Local Logon (used to log on directly to a system) :** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**
- User identification and local authentication (at least passwords) is required for all user ID's.

**User Authentication: Remote Logon (access a second system from the first without invoking a second authentication):** User authentication is the process by which the system verifies the user's claim of identity. The user presents some piece of information to the system that is his/hers; something known (password), possessed (key or token) or is (biometrics measurement).
**Template Section 5.7**
**Security Requirements**
- Remote authentication is permitted at the discretion of the remote system admin when the authenticating system meets all security requirements of the remote system, audit trails are created, and the risk of subverting the connection is acceptable.

**Failed Logon Attempts:** Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination. Excessive failed logon attempts may indicate that an unauthorized user is attempting to access the system.
**Template Section 5.7 and 5.8**
**Security Requirements**
- The user ID owner is notified of failed logon attempts.
- The user ID is suspended, by system intervention, after five or fewer unsuccessful logon attempts or provides some form of system evasive action.
- The log of unsuccessful logon attempts is reviewed weekly.

**Controlled Access Protection:** Controlled access protection is the ability of the system to control which users have access to resources. Ensure that all systems accessed will provide controlled access protection when users are not authorized for all information on the system.
**Template Sections 5.7 and 5.8**
**Security Requirements**

- The system provides individual electronic accountability through identification and authentication of each system user.
- The system provides the ability to control a user's access to information.
- The system provides audit trails or a journal of security-relevant events.

**Default File Protection:** Default file protection is the access control the system places on a file when the data owner does not take explicit action.

**Template Section 5.7**

**Security Requirements**

- System default file protection parameters are set to grant write and execute access to the file owner and to necessary operating system components.

**Data Owner Requirements/Responsibilities:** An application processes data, giving it meaning. An application derives its sensitivity from the data it processes or contains. A computer derives its sensitivity from the applications it handles. Data owners determine sensitivity.

**Template Sections 1.4 and 2**

**Security Requirements**

- The data owner has identified authorized users and custodians.
- The information category or sensitivity of the application/information is specified by the data owner.
- The data owner has identified and protected private data from unauthorized disclosure.
- The security protections to be implemented have been specified by the data owner.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.

**Template Sections 5.3 and 7**

**Security Requirements**

- All workstation software not acquired through the normal procurement processes will be approved before installation in accordance with established requirements.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.

**Template Section 1.4**

**Security Requirements**

- Operational security controls are reviewed and enforced.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.
- Security requirements are established for applications.

**Multiuser Workstations**

**Security Requirements**

- A contingency plan is developed.

- Backup requirements are established.
- Virus detection software is installed in the workstation where applicable.
- System configuration is documented.

## III. Singleuser Workstation

A single-user workstation is one that may be used by only one person at a time, though many people have access.

**Individual Accountability**
**Template Section 7**
**Security Requirements**

- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.
- Individuals are held accountable for the protection against loss or disclosure of password they possess.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not the name of a vendor product or a nickname for a product.
- The password is not equal to the user ID.
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.
- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password expires after 1 year maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.
- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant ongoing access to another individual or may create a temporary password.

**Password Storage**
**Template Section 5.7**
**Security Requirements**

- Stored passwords are protected in such a way that only the password system is authorized access to a password.
- Passwords that are encrypted before that are stored are protected from substitution (I.e., protection is provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

**Password Distribution**
**Template Section 5.7**
**Security Requirements**

- Passwords are distributed so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel.
- Personal passwords are distributed in a way that affords reasonable protection from unauthorized disclosure.
- Passwords are distributed in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system.
- Passwords are not visible at the user terminal when being typed.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.
- The policy ensures that positive identification of the user ID owner is provided.
- A new nontrivial password is assigned at the user's request.
- The password is reset by the user during the first sign-on.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password assignment is nontrivial.
- The initial user password is changed during the first logon by the user.
- All vendor-supplied passwords are removed.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.
**Template Sections 5.3 and 7**
**Security Requirements**

- All workstation software not acquired through the normal procurement processes will be approved before installation in accordance with established requirements.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.

**Template Section 1.4**

**Security Requirements**

- Security requirements are established for applications.
- Decisions on implementation of security controls are reviewed during definition, design, programming and testing.
- Operational security controls are reviewed and enforced.

**Single User Workstations**

**Security Requirements**

- Virus detection software is installed on all applicable workstations.
- A risk management program commensurate with the information category/sensitivity level is implemented.
- Backup and recovery requirements are established.

## Baseline Security Requirements for Systems Rated Public Access (PUB)

## I. Servers and Mainframes

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual is terminated **for cause or because of reduction in force.**
**Template Section 5.6**
**Security Requirements**

- The user ID is removed within 2 working days of the termination.

**Notification Upon Termination:** A user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual has **resigned, received a change of job, or has retired**, and no longer requires access to the system to perform assigned duties.
**Template Section 5.6**
**Security Requirements**

- The user ID is removed within 15 working days.

**Individual Accountability**
**Template Section 7**
**Security Requirements**

- Individuals are held accountable for the protection against loss or disclosure of password they possess.
- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.
- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).
- The password is not equal to the user ID.
- The password is not the name of a vendor product or a nickname for a product.

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**

**Security Requirements**

- The password expires after 1 year maximum.

**Password Sharing**
**Template Sections 5.7 and 7**
**Security Requirements**

- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.
- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant ongoing access to another individual or may create a temporary password.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.
- The policy ensures that positive identification of the user ID owner is provided.
- A new nontrivial password is assigned at the user's request.
- The password is reset by the user during the first sign-on.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- The initial user password is changed during the first logon by the user.
- All vendor-supplied passwords are removed.
- The initial user password assignment is nontrivial.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.
**Template Sections 5.3 and 7**
**Security Requirements**

- All mainframe public domain software not acquired through the normal procurement processes will be approved before installation in accordance with established requirements.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.
**Template Section 1.4**
**Security Requirements**

- Operational security controls are reviewed and enforced.

**Password Encryption**
**Template Sections 5.4**
**Security Requirements**

- Passwords are encrypted if the system on which they are used is connected to a system of higher sensitivity.

**Documentation:** Centralized operations refer to tasks that support multiuser systems, such as the operation and monitoring of console control units and peripherals, job scheduling, media retention and accountability, job quality control, etc.
**Template Section 5.5**
**Security Requirements**

- Applications are reviewed annually for changes in information categories/sensitivity level.
- A list of personnel responsible for system and application software is maintained.

**Privileged Operations**
**Template Sections 5.5, 5.7, and 5.8**
**Security Requirements**

- IT security incidents are documented and reported to the Computer Security Official or POC and management.
- Access to operator consoles is controlled.
- Operators do not transfer privileged activity outside the operations area without proper authorization.

**Console Logon**
**Template Sections 5.5, 5.7, and 5.8**
**Security Requirements**

- Only the operations group is authorized to disable console logging and that the event is logged when performed.
- Operator console logs are reviewed regularly.
- Only the operations group is authorized to disable console logging and that the event is logged when performed.
- IT security incidents are documented and reported to the Computer Security Official or POC and management.

**Media Storage**
**Template Section 5.1**
**Security Requirements**

- Media is protected from theft, vandalism, and natural disasters.

**Authentication Requirements:** Authentication is the process by which a computer verifies the identity of a user. The process generally consists of the computer prompting for a user ID and, at minimum, a password.
**Template Section 5.7**
**Security Requirements**

- Network devices detect and close broken sessions.

- Dial-in diagnostics that bypass normal authentication when they are not in use are disabled as directed by management.

**File Transfer and Remote Logon Protection Requirements:** Services provided by the network include such processes as file transfer and remote logon.
**Template Sections 5.6 and 5.7**
**Security Requirements**

- Inbound or outbound file transfer from unauthenticated users is allowed only to a restricted set of directories.
- Access to any privileged network software is restricted to authorized users.
- Proxy or trusted logons are restricted as directed by management.

**Connection Requirements:** Network attachment increases the number of threats to which a system may be vulnerable. Therefore, certain security precautions must be taken before a system is attached to a network.
**Template Section 5.3**
**Security Requirements**

- Network connections have been evaluated according to local IT security policies, procedures and guidance.

## II. Multiuser Workstations

A multiuser workstation, also known as a host system, is one that can be accessed simultaneously by other workstations.

**Individual Accountability**
**Template Section 7**
**Security Requirements**

- Individuals are held accountable for all activity that occurs as a result of deliberately revealing his or her user ID and password.
- Individuals are held accountable for the protection against loss or disclosure of password they possess.

**Password Length and Composition**
**Template Sections 5.7 and 7**
**Security Requirements**

- Passwords have a minimum of eight characters.
- The eight characters contain at least one character each from at least three of the following: uppercase letters, lowercase letters, numbers, special characters.

**Password Triviality**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password is not the name of a vendor product or a nickname for a product.
- The password is not equal to the user ID.
- The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.

- The password is not either wholly or predominantly composed of personal information (family's or pet names, SSN, contractor, division or branch name, repetitive or keyboard patterns, automobile or sport team names).

**Password Maximum Lifetime**
**Template Sections 5.7 and 7**
**Security Requirements**

- The password expires after 1 year maximum.

**Password Sharing**
**Template Sections 5.7 and 7**

- The user ID owner may employ system features (e.g., LOGONBY or the equivalent) to grant ongoing access to another individual or may create a temporary password.
- Personal passwords used to authenticate identity are owned (known) only by the individual having that identity.

**Password Reset**
**Template Sections 5.7 and 7**
**Security Requirements**

- The policy ensures that positive identification of the user ID owner is provided.
- A new nontrivial password is assigned at the user's request.
- The password is reset by the user during the first sign-on.
- The policy ensures that the name, location, phone number, and system user ID of the user needing reset is confirmed.

**Initial Password**
**Template Sections 5.7 and 7**
**Security Requirements**

- All vendor-supplied passwords are removed.
- The initial user password assignment is nontrivial.
- The initial user password is changed during the first logon by the user.

**Public Domain Software:** Public domain software is when the source takes no responsibility for the integrity or maintenance of the software. It is often written by enthusiasts and distributed via e-mail, bulletin boards, Usenet, etc. It is a common carrier of malicious code.
**Template Sections 5.3 and 7**
**Security Requirements**

- All workstation software not acquired through the normal procurement processes will be approved before installation in accordance with established requirements.

**Formalized Project Life-Cycle Development:** Software that is developed or customized by either in-house or contractor-supplied services, including universities. Those engaged in formal life-cycle project development must ensure that basic security is integrated throughout the software's life-cycle.
**Template Section 1.4**

**Security Requirements**

- Operational security controls are reviewed and enforced.

**Multiuser Workstations**

**Security Requirements**

- Backup requirements are established.
- System configuration is documented.
- Virus detection software is installed in the workstation where applicable.

# Attachment B. Sample Rules of Behavior

## Rules of Behavior for Use of Computer Systems

The rules listed below are for the use of Information Technology (IT) resources operated by personnel assigned to the XYZ Security Behavioral Corporation. The purpose is to increase individual awareness and responsibility, and to ensure that all users use the IT resources in an efficient, ethical, and lawful manner.

I, (please print)_____, understand that:

1. The computer system I am requesting an account for may only be used for official purposes in the conduct of my duties.
2. All software on the computer system is protected in accordance with NASA and Federal Government security and control procedures which will be adhered to. Licensed software will only be used in accordance with the license.
3. Use of these IT resources gives consent for monitoring and security testing to ensure proper security procedures and appropriate usage are being observed.
4. Electronic communications facilities (such as e-mail and Netnews) are for authorized business use only. IT resources will not be used for fraudulent, harassing or obscene messages and/or materials.
5. When access is no longer required to these IT resources, I must notify appropriate responsible parties and make no further attempt to access these resources.
6. Dial-up accounts are a government computer resource for use by government employees and approved contractors and is to be used only for government related work. If it is discovered that resources are being misused, the dial-up account will be deleted and further appropriate action may be taken.
7. No IT resources will be removed without a property pass from the property custodian.
8. Fixed media will be erased prior to transferring the IT resources or designating the resource for excess.
9. Tampering with another user's account, files, or processes without the other user's express permission.
10. Use of the system resources for personal purposes; or other unauthorized activities is strictly prohibited and will result in disciplinary action.
11. Logon ID's and passwords may never be transferred or shared for any reason.
12. Active logons should never be left unattended. Workstations will be paused when unattended for short periods of time (less than 30 minutes).
13. Do not logon to more than one workstation/terminal unless each can be kept under constant surveillance.
14. Passwords:
    a. will be a minimum of 8 alphanumeric characters.
    b. will be changed at least every 180 days
    c. will not be a word appearing in an English or foreign dictionary
    d. will be memorized and not written down

    e. will not be stored in keyboard macros or .bat files
    f. will not consist of personal ID data or be easily guessable
15. Challenge anyone in the computer facility who does not have an appropriate badge.
16. Rooms with workstations or terminals must be locked after normal working hours except when such workstations or terminals are located in continuously manned operational areas.
17. Access to and use of the Internet will only be for official purposes in the conduct of your duties.
18. Personally owned, provided, or downloaded software may not be installed without management approval.
19. E-mail will only be used for official purposes and will not be used to transmit the following information:
    a. U.S. Government or corporate credit card numbers
    b. Designated Sensitive Data
    c. Risk Assessments
    d. For Official Use Only information
    e. Privacy Act Data
    f. Proprietary Data
    g. Procurement Sensitive Data
    h. Source Evaluation Board (SEB) information
20. Any unauthorized penetration attempt, unauthorized system use, or virus activity will be reported to your supervisor.

Failure to adhere to these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Signing the front of this form indicates that you have read, understand, and will comply with these rules.

I understand that failure to abide by these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.
I have read and understand these Rules of Behavior for the XYZ Security Behavioral Corporation information technology systems and agree to abide by them.
I fully understand my responsibilities as a user of this system/network.

User Name: (please print)_____

User Signature:_____

Organization Code/Contractor Name:_____

Date: _____

# Attachment C: Sample Authorization to Process Letter

## EOSDIS SECURITY AUTHORIZATION TO PROCESS LETTER

To: ESDIS Organization Computer Security Official (CSO)

From: (Line Manager and Name of System/Network/Facility)

Date: (Month, Day, Year)

Subj.: Authorization to Process

In accordance with Office of Management and Budget (OMB) Circular No. A-130, Appendix III, and NASA Procedures and Guidance for the Security of Information Technology (NPG) 2810, I certify that (name of system/network/facility) is compliant with the following security requirements and minimum security controls are in place prior to authorizing the system for processing:

- IT Security Plan for the system is completed, updated, and reviewed.
- IT Security Contingency Plan is completed and tested.
- ESDIS Network Security Assessment is completed.
- Risk Assessment Plan is completed.
- Rules of Behavior of the system are established and signed by users.
- Review of the security controls of the systems is completed.
- In-place and planned security safeguards appear to be adequate and appropriate for the system.

Adequate security controls and procedures have been implemented commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of this Federal Information Technology Resource.

I therefore accept all security risks involved in operating the (name of system/network/facility) and authorize it to process data effective (Month Day, Year).

Name _____

Signature _____

Title _____

Organization Code _____